UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/903,278	07/11/2001	Philip M. Walker	10012790-1	9299

7590 03/01/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
TRAN, TONGOC	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/903,278	WALKER ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on December 5, 2006. Claims 1-26 are pending.

Response to Arguments

2. Applicant's arguments filed on December 5, 2006 have been fully considered but they are not persuasive.

Applicant contends that the cited prior art, Schneier, does not teach the probe (audit logging program) is operable to "execute" in the target (remarks, page 6). Examiner asserts that Schneier's audit logging program met the claimed limitation because an audit logging program performs a functionality of enabling the program to probe (record or audit) a predetermined data. The difference between a data file which is stored in a memory would always remains to be a data file whereas a program that record or audit information is a program operable to execute or to perform certain functionality. Applicant argues that the cited "target" in the claim teaches an untrusted computer whereas Schneier appears to disclose a trusted computer. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., untrusted computer) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claimed language recites "a target" which can broadly interpreted to be any computer system

that is being audited or probed. Even if the language would have recited "untrusted computer" instead of "the target", Schneier's determining step to verify whether the predetermined data (audit log) has been altered would still have met the claimed language because the fact that the verification is necessary to ensure the data has not been altered suggests an environment that is not secure.

In response to Applicant's argument that SOM's process (or monitor) compare an attack signature to training signatures taught by Hill fails to teach the claimed limitation of "to determine whether the target has been altered" (remark page 8). Examiner asserts that the step of comparing the received signature with the training signature taught by Hill encompasses reading, comparing and determining the differences in the set of received data with another set of predetermined data. Therefore, it met the claimed limitation of "to determine whether the target has been altered".

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-17, 19-24 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier et al. (U.S. Patent No. 5,978,475).

In respect to claims 1, 10 and 19, Schneier discloses a system and method comprising:

a target; a probe operable to execute in the target and collect a predetermined set of data associated with the target; and a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered (e.g. col. 6, line 41-col. 7, line 19, target, untrusted computer, monitor-trusted computer, a probe-audit log, "transmit it to the trusted computer for verification", "verification-the set of operations done on the logfile to guarantee that it hasn't been altered...", col. 7, lines 14-19).

In respect to claims 2, 11 and 20, Schneier further discloses wherein the probe is resident in the target (e.g. col. 7, lines 5-13).

In respect to claims 3, 12 and 21, Schneier further discloses wherein the monitor is operable to send the probe to the target for execution (e.g. col. 7, lines 5-6).

In respect to claims 4, 13 and 22, Schneier further discloses wherein the probe repeatedly executes and the predetermined set of data varies for each execution of the probe (e.g. col. 7, lines 7-8).

In respect to claim 5, Schneier further discloses wherein the predetermined set of data includes system attributes and system usage data (e.g. col. 1, lines 34-52 and col. 6, lines 51-64).

In respect to claims 6 and 15, Schneier further discloses wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe (e.g. col. 8, line 45-col. 9, line 2).

In respect to claims 7 and 16, Schneier further discloses wherein the monitor is operable to compare the calculated signature value to an expected signature value (e.g. col. 8, line 45-col. 9, line 2).

In respect to claims 8, Schneier further discloses wherein the probe is operable to determine a signature value of a random subset of an execution image of the probe (e.g. col. 18, lines 23-28).

In respect to claims 9 and 17, Schneier further discloses wherein the probe is operable to generate an encryption key from the signature value for encrypting the collected predetermined set of data (e.g. col. 8, line 45-col. 9, line 2).

In respect to claims 19 and 26, Schneier further discloses receiving collected data encrypted by the probe using an encryption key derived from a self-hash value, the data including system attribute data and system usage data; from a self-hash value, the data including system attribute data and system usage data; decrypting the encrypted data; and verifying the system attribute data (e.g. Col. 1, lines 34-52, col. 5, lines 5-20, col. 6, line 51-col. 7, line 19 and col. 8, line 45-col. 9, line 3).

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 10 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al. (U.S. Patent No. 6,088,804).

In respect to claims 1, 10 and 19, Hill discloses a system and method comprising:

a target; a probe operable to execute in the target and collect a predetermined set of data associated with the target; and a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered (e.g. col. 3, lines 1-16, col. 4, lines 30-41, security agent-probe, security event-set of data items associated with the target, col. 5, lines 46-52, col. 4-22, node-target, agents send info. for collection and comparison).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 18 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,978,475).

In respect to claims 18 and 25, Schneier further discloses sending the encrypted data to a monitor, the data including system attribute data and system usage data; Decrypting the encrypted data using a decryption key; Verifying the system attribute data; and (e.g. Col. 1, lines 34-52 and col. 6, line 51-col. 7, line 19, col. 8, line 45-col. 9, line 3). Schneier does not disclose generating billing data based on the system usage data in response to the system attribute data being verified. However, Office Notice is taken that generating billing according to system usage is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement security audit logging and verifying operation taught by Schneier to generate billing according to the information for billing purposes.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
PRIMARY EXAMINER

February 22, 2007